Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 4: Definities en Afkortingen

Datum 18 januari 2016

Colofon

Versienummer 4.2
Contactpersoon Policy Authority PKIoverheid

Organisatie Logius

Bezoekadres
Wilhelmina van Pruisenweg 52

Postadres
Postbus 96810
2509 JE DEN HAAG

T 0900 - 555 4555
servicecentrum@logius.nl

Inhoud

De Policy Authority (PA) van de PKI voor de overheid ondersteunt de Minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid.

De PKI voor de overheid is een afsprakenstelsel. Dit maakt generiek en grootschalig gebruik mogelijk van de elektronische handtekening, en faciliteert voorts identificatie op afstand en vertrouwelijke communicatie. De taken van de PA PKIoverheid zijn:

- het leveren van bijdragen voor de ontwikkeling en het beheer van het normenkader dat aan de PKI voor de overheid ten grondslag ligt, het zogeheten Programma van Eisen (PvE);
- het proces van toetreding door Certification Service Providers (CSP's) tot de PKI voor de overheid begeleiden en voorbereiden van de afhandeling;
- het toezicht houden op en controleren van de werkzaamheden van CSP's die onder de root van de PKI voor de overheid certificaten uitgeven.

De doelstelling van de Policy Authority is:
Het handhaven van een werkbaar en betrouwbaar normenkader voor PKI-diensten dat voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en transparant is voor de gebruikers.

Revisiegegevens

Versie	**Datum**	**Omschrijving**
1.0	09-11-2005	Vastgesteld door BZK november 2005
1.1	25-01-2008	Vastgesteld door BZK januari 2008
1.2	13-01-2009	Vastgesteld door BZK januari 2009
2.0	09-10-2009	Vastgesteld door BZK oktober 2009
2.1	11-01-2010	Wijzigingen naar aanleiding van naamswijziging GBO.Overheid in Logius
3.0	25-01-2011	Vastgesteld door BZK januari 2011
3.1	01-07-2011	Vastgesteld door BZK juni 2011
3.2	27-01-2012	Vastgesteld door BZK januari 2012
3.3	01-07-2012	Vastgesteld door BZK juni 2012
3.4	04-02-2013	Vastgesteld door BZK januari 2013
3.5	06-07-2013	Vastgesteld door BZK juni 2013
3.6	27-01-2014	Vastgesteld door BZK januari 2014
3.7	06-2014	Vastgesteld door BZK juni 2014

4.0	12-2015	Vastgesteld door BZK december 2014
4.1	07-2015	Vastgesteld door BZK juli 2015
4.2	01-2016	Vastgesteld door BZK januari 2016

1 Inleiding

1.1 Programma van Eisen

Dit is deel 4 van het Programma van Eisen (PvE) van de PKI voor de overheid. In het PvE zijn de normen voor de PKI voor de overheid vastgelegd. Dit deel heeft betrekking op de definities en afkortingen die binnen de PKI voor de overheid worden gehanteerd.

In dit deel worden de termen en afkortingen verklaard die worden gebruikt in delen 1 t/m 3 van het PvE. De belangrijkste doelstelling van het vermelden van deze definities en afkortingen is het scheppen van duidelijkheid omtrent de door de PA gebruikte terminologie. Tevens kan dit deel dienst doen als referentiedocument binnen de Nederlandse overheid voor PKI gerelateerde zaken.

1.2 Status

Dit is versie 4.2 van deel 4 van het PvE. De huidige versie is bijgewerkt tot en met 18 januari 2016.

De PA heeft de grootst mogelijke aandacht en zorg besteed aan de gegevens en informatie, die zijn opgenomen in dit deel van het PvE. Desalniettemin is het mogelijk dat onjuistheden en onvolkomenheden voorkomen. De PA aanvaardt geen enkele aansprakelijkheid voor schade als gevolg van deze onjuistheden of onvolkomenheden.

1.3 Gevolgde Werkwijze

De volgende werkwijze is bij het maken van dit document gevolgd.

Wanneer er in de Nederlandse wetgeving een definitie is voor een bepaald begrip, dan is deze definitie gehanteerd. Daar waar deze definitie een algemeen karakter heeft die voor onze doeleinden niet toereikend is, wordt tevens een aanvulling vermeld. Gebruikt zijn hierbij: De Telecommunicatiewet (dossier 25533) en de wet elektronische handtekeningen (dossier 27743). In het document is dit weergegeven door het betreffende wetgevingsdocument onderstreept weer te geven tussen [ ].
Daar waar deze niet in tegenspraak is met de Nederlandse wetgeving, zijn de begrippen uit de Nederlandstalige vertaling van de Europese Richtlijn voor elektronische handtekeningen (richtlijn 1999/93/EG) gebruikt. Wanneer een definitie hieruit is gebruikt, wordt dit in het document onderstreept aangegeven tussen [ ].

Vervolgens zijn de documenten gebruikt van internationale organisaties die zich bezighouden met standaardisatie en dan met name op het gebied van elektronische handtekeningen. Hierbij doen zich enige complicaties voor:

- Niet alle documenten gebruiken dezelfde definities. Daar waar dit zo is, gebruiken wij de publicaties van officiële Europese standaardisatieorganisaties zoals CEN en ETSI en niet zozeer die van bijvoorbeeld IETF of NIST.
- Van de betreffende documenten bestaan geen officiële Nederlandse vertalingen. Er zijn wel Nederlandse organisaties die ze hebben vertaald, maar deze vertalingen wijken onderling soms sterk af. In dit document is ervoor gekozen om de originele formulering zelf te vertalen naar Nederlands.
- De meeste beschikbare documenten beschouwen alleen regels voor elektronische handtekeningen. In het model van de PKI voor de overheid worden nog andere certificaten in beschouwing genomen. Dat betekent dat sommige begrippen in het model van de PKI voor de overheid niet één op één overgenomen kunnen worden vanuit het beperktere model. In dit document is ervoor gekozen om zoveel mogelijk daar waar de afwijking slechts enkele woorden betreft, dit direct toe te passen. Daar waar de wijziging aanzienlijk meer bedraagt, is de oorspronkelijke tekst weergegeven, aangevuld met een toelichting.
- Veel termen worden in de vakliteratuur afgekort vanuit het Engels. Deze afkortingen, of soms zelfs de Engelse woorden die daaraan ten grondslag lagen, zijn inmiddels in vakkringen verregaand ingeburgerd. In deze definitielijst is ook deze praktische benadering gevolgd. In die gevallen waar voor een gebruikte Engelstalige term een Nederlandse term bestaat in de Europese Richtlijn of de wet elektronische handtekeningen, is deze Nederlandse term tussen () weergegeven.
- Voor de spelling zijn het VanDale woordenboek en de "Woordenlijst Nederlandse taal" inclusief de spellingsregels gevolgd.

1.4 Gebruik

Wanneer bij een definitie een doorverwijzing staat naar een andere definitie, dan dient deze laatste gebruikt te worden. Daar waar een verkorte vorm (bijvoorbeeld een afkorting) achter een definitie staat, dan geniet de verkorte vorm in enkele gevallen de voorkeur. Ter verduidelijking is de term die de voorkeur heeft onderstreept. In dit document zelf worden de afkortingen alleen bij hun eigen uitleg gebruikt tenzij het gaat om namen van technieken of organisaties. Een uitzondering is gemaakt voor CSP, aangezien deze afkorting reeds verregaand is ingeburgerd.

Daar waar een letterlijke tekst uit de Telecomwet, de Wet elektronische handtekeningen, het Besluit elektronische handtekeningen of de Europese Richtlijn is weergegeven, wordt dit als zodanig expliciet vermeld. Tevens wordt de letterlijke tekst zelf cursief en in een kleiner lettertype weergegeven.

2 Definities

Aanvrager
Een natuurlijke of rechtspersoon die een aanvraag tot uitgifte van een certificaat indient bij een Registration Authority.

Abonnee (E: Subscriber)
Een natuurlijke persoon of rechtspersoon die partij is bij een overeenkomst met een aanbieder van openbare telecommunicatiediensten voor de levering van dergelijke diensten. [Telecomwet]

In het kader van de PKI voor de overheid:
Een abonnee gaat een overeenkomst aan met een CSP namens één of meer certificaathouders. Hóe de levering van certificaten door de CSP aan die certificaathouders plaatsvindt, regelen de abonnee en de CSP onderling. In het domein Burger zijn abonnee en certificaathouder altijd dezelfde partij.

Accreditatie
Procedure waarbij een autoriteit bezittende organisatie een formele erkenning uitspreekt dat een entiteit bekwaam is specifieke taken uit te voeren.

Advanced electronic signature
Zie "Geavanceerde elektronische handtekening".

Advanced Encryption Standard – AES
De nieuwe, door de NIST vastgestelde en voor de Verenigde Staten geldige, standaard voor het vercijferen van data. De AES dient als opvolger van het veel gebruikte DES algoritme en in mindere mate voor het SHA-1 algoritme. De AES maakt gebruikt van het in België ontwikkelde Rijndael algoritme.

Afhankelijkheids- en Kwetsbaarheidsanalyse – A&K-analyse
De analyse die wordt uitgevoerd met als doel het vaststellen van het vereiste beveiligingsniveau waardoor een betrouwbare communicatie binnen de infrastructuur van de PKI voor de overheid wordt gewaarborgd.

Algoritme
Een verzameling instructies die stap voor stap uitgevoerd dienen te worden om een rekenkundig proces uit te voeren of een specifiek type problemen op te lossen.

Application Programming Interface - API
Een geformaliseerde verzameling van aanroepen en routines die door een applicatie worden uitgevoerd om gebruik te maken van ondersteunende diensten (bijvoorbeeld een netwerk).
In relatie met PKI zijn het de aanroepen vanuit de applicaties die gebruik maken van cryptografische handelingen (versleutelen, tijdstempelen, et cetera).

Asymmetrisch sleutelpaar
Een publieke en private sleutel binnen de public key cryptografie die wiskundig met elkaar zijn verbonden zodanig dat de publieke sleutel en de private sleutel elkaars tegenhanger zijn. Wordt de ene sleutel gebruikt om te versleutelen, dan móet de andere gebruikt worden om te ontsleutelen en omgekeerd.

Attribuut
Informatie behorende bij een object (persoon of entiteit) die een kenmerk van die entiteit specificeert, zoals groepslidmaatschap, een rol of andere autorisatie-informatie verbonden met de houder van een hiervoor uitgegeven attribuutcertificaat.

Attribuutcertificaat (E: Attribute Certificate)
Een datastructuur die een verzameling van attributen voor een eindgebruiker plus aanvullende informatie bevat en die getekend is met de private sleutel van de AA die het certificaat uitgegeven heeft.

Attribute Authority – AA (NL: Attribuut Autoriteit)
Een autoriteit die privileges toekent door attribuutcertificaten uit te geven en te tekenen. De Attribute Authority is gedurende de gehele lifecycle van de attribuutcertificaten daar verantwoordelijk voor, niet alleen wanneer ze geregistreerd worden.

Authenticatie
1. Het controleren van iemands identiteit, voordat informatieoverdracht plaatsvindt.
2. Het controleren van de juistheid van een boodschap of afzender.

In de Wet EH wordt de term "Authentificatie" gebruikt. Het oorspronkelijke Engelstalige woord is "Authentication". In alle technische vakliteratuur wordt dit echter vertaald met "Authenticatie". In dit document wordt dit laatste dan ook gehanteerd.

Authenticiteitcertificaat
Een certificaat dat, afhankelijk van de specifieke toepassing, wordt gebruikt voor authenticatie of elektronische identificatie.

Authentificatie
Zie "Authenticatie".

Autonome Apparatencertificaat
De certificaathouder is een apparaat waarvan de werking en de wijze van produceren aantoonbaar conformeren aan het normenkader van een specifieke soort autonome apparaten en dat in die hoedanigheid door de kadersteller geautoriseerd is gebruik te maken van een aan dat apparaat gekoppeld Autonome Apparatencertificaat.

Autoriseren
Het verlenen van een bevoegdheid tot het verrichten van handelingen (zoals inzien, aanpassen of bewerken) op informatie of middelen.

Beleidsregel aanwijzing certificatieorganisaties elektronische handtekeningen
De beleidsregel die tegelijkertijd met de wet EH van kracht is geworden. De beleidsregel betreft de aanwijzing van organisaties die certificatiedienstverleners toetsen op de overeenstemming met de bij of

krachtens de Telecommunicatiewet gestelde eisen, op grond van artikel 18.16 van de Telecommunicatiewet.

Beroepsgebonden certificaathouder
De certificaathouder is een beoefenaar van een erkend beroep en in die hoedanigheid zelf een abonnee en daarmee de contracterende partij.
In PvE deel 3a bij 3.2.5-pkio29 staat dat "Als authentiek bewijs voor het uitoefenen van een erkend beroep wordt alleen beschouwd:

a. ofwel een geldig bewijs van inschrijving in een door de betreffende beroepsgroep erkend (beroeps)register waarbij een wettelijk geregeld tuchtrecht van toepassing is;
b. ofwel een benoeming door een Minister;"

Met betrekking tot deze twee voorwaarden gaat hem om de volgende beroepen (dit betreft een limitatieve lijst):
1. Accountant-Administratieconsulent;
2. Advocaat;
3. Octrooigemachtigde;
4. Registerloods;
5a. Degenen die zijn ingeschreven in een register als bedoeld in artikel 3 van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG).
5b. Degenen die een beroep uitoefenen waarvan de opleiding krachtens artikel 34, eerste lid, van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) is geregeld of aangewezen.
6. Notaris;
7. Kandidaat notaris
8. Toegevoegd notaris;
9. Gerechtsdeurwaarder;
10. Waarnemend gerechtsdeurwaarder;
11. Toegevoegd kandidaat gerechtsdeurwaarder;
12. Octrooigemachtigde;
13. Registeraccountant;
14. Dierenarts;
15. Zeevarende;
16. (Hoofd) Bewaarder;
17. Gemandateerd bewaarder;
18. Technisch medewerker schepen;
19. Inspecteur Scheepsregistratie;
20. Belastingdeurwaarder;
21. Rijksdeurwaarder.

Beschikbaarheid
Het aanwezig zijn en het toegankelijk zijn van de relevante gegevens. Wat betreft infrastructuur: de mate waarin een systeem bruikbaar is op het moment dat hier een behoefte aan bestaat.

Besluit EH
Het besluit elektronische handtekeningen dat als Algemene Maatregel van Bestuur (AmvB) tegelijkertijd met de wet EH van kracht is geworden. Het besluit stelt de eisen vast voor het verlenen van diensten voor elektronische handtekeningen. Nr. WJZ/03/02264.

Bevoegd vertegenwoordiger
Een natuurlijk persoon die bevoegd is een organisatie te vertegenwoordigen. Bevoegdheid tot vertegenwoordiging kan voortvloeien uit de wet of uit een volmacht. Er kan ook sprake zijn van meerdere natuurlijk

personen, b.v. een bestuur van een vereniging, die bevoegd zijn een organisatie te vertegenwoordigen.

In onderstaand schema volgt een beschrijving wie *normaliter* bevoegd is om een bepaalde organisatie te vertegenwoordigen:

Organisatie	Vertegenwoordigingsbevoegd
Gemeente	Burgemeester Gemeente secretaris
Provincie	Commissaris van de Koning
Ministerie	Minister Directeur Generaal Secretaris Generaal
School	Directeur/Hoofd Secretaris van het bestuur
Waterschap	Directeur (Dijkgraaf) Bestuurder(s)
Zorginstelling	Directeur Bestuurder(s)
Vereniging	Bestuurder(s)
BV	Bestuurder(s)
NV	Bestuurder(s)
Maatschap	Alle maten of één der maten als vertegenwoordiger van de maatschap (d.w.z. als vertegenwoordiger van alle maten gezamenlijk) als deze door de andere maten hiertoe is gevolmachtigd.
Eenmanszaak	Eigenaar
Vennootschap onder Firma (VOF)	Iedere vennoot, die daarvan niet is uitgesloten, is bevoegd om 'ten name van de vennootschap' (d.w.z. de gezamenlijke vennoten) te handelen
Commanditaire vennootschap	Alleen beherende vennoten: zij zijn bevoegd om namens de commanditaire vennootschap op te treden en zij zijn hoofdelijk verbonden voor de in naam van de vennootschap aangegane verbintenissen.
Coöperatie	Bestuurder(s)
Baten-lastendienst	Directeur Bestuurder(s)
Zelfstandig bestuursorgaan (ZBO)	Directeur Bestuurder(s)

Biometrie
Een techniek voor persoonsherkenning of verificatie aan de hand van een uniek lichamelijk kenmerk. Bijvoorbeeld: irisscan, vingerafdrukscan, gezichtsherkenning.

Blanco kaarten
Kaarten (met name smartcards) die grafisch zijn voorbedrukt, maar nog niet zijn voorzien van sleutelmateriaal of persoonsgegevens.

Bridge Certification Authority – Bridge-CA
Een Certification Authority die als spil dient in een netwerk van elkaar erkennende Certification Authorities die interoperabel zijn. Deze Certification Authority slaat dus als het ware een brug tussen de diverse Certification Authorities.

CA-certificaat
Een certificaat van een Certification Authority. Binnen de PKI voor de overheid is een bijzonder geval hiervan het CA-certificaat van de CSP-CA, dat door de Policy Authority wordt uitgegeven. Dit certificaat wordt het CSP-certificaat genoemd. Zie ook het plaatje bij "Hiërarchisch model".

CA-signing
Het ondertekenen van een CA-certificaat. Dit kan het geval zijn wanneer een CA binnen de hiërarchie wordt aangemaakt. Ook bij cross-certification vindt dit plaats, in feite is er daar sprake van wederzijdse CA-signing. Zie ook het plaatje bij "Hiërarchisch model".

Calamiteit (E: Disaster)
Een ongeplande situatie waarbij verwacht wordt dat de duur van het niet beschikbaar zijn van één of meer diensten de afgesproken drempelwaarden zal overschrijden.

CEN Workshop Agreement - CWA
Een document van de Comité Européen de Normalisation (CEN) met daarin adviezen en voorstellen voor Europese standaardisatie. In vergelijking met de totstandkoming van een ETSI-norm, verloopt de totstandkoming van een advies van de CWA sneller. Daarentegen is een ETSI-norm meer te beschouwen als officieel uitgangspunt.

Certificaat
Een elektronische bevestiging die gegevens voor het verifiëren van een elektronische handtekening met een bepaalde persoon verbindt en de identiteit van die persoon bevestigt. [Wet EH]
In het kader van de PKI voor de overheid:
De publieke sleutel van een eindgebruiker, samen met aanvullende informatie. Een certificaat is vercijferd met de private sleutel van de Certification Authority die de publieke sleutel heeft uitgegeven, waardoor het certificaat onvervalsbaar is. Zie ook het plaatje bij "Hiërarchisch model".

Certificaat & kaart management
De procedures met betrekking tot het beheer van de certificaten en smartcards.

Certificaat identifier – Certificaat-ID
De unieke aanduiding van een certificaat bestaande uit de naam van de Certification Authority en uit het door de Certification Authority toegewezen serienummer.

Certificaatgeldigheidsduur (E: Certificate validity period)
Het tijdsinterval gedurende welke de Certification Authority de bruikbaarheid van het certificaat garandeert. De Certification Authority

houdt tot ten minste 6 maanden na het verlopen van de geldigheidsduur informatie bij betreffende de status van een certificaat.

Certificaathouder
Een entiteit die geïdentificeerd wordt in een certificaat als de houder van de private sleutel behorend bij de publieke sleutel die in het certificaat gegeven wordt.
De certificaathouder zal in het geval van persoonsgebonden certificaten een natuurlijke persoon zijn, in het geval van services certificaten zal de certificaathouder een functie of een machine/server zijn. In het domein Burger zijn certificaathouder en abonnee altijd dezelfde partij.

Certificaatprofiel
Een beschrijving van de inhoud van een certificaat. Ieder soort certificaat (handtekening, vertrouwelijkheid, e.d.) in ieder domein heeft een eigen invulling en daarmee een eigen beschrijving. Hierin staan bijvoorbeeld afspraken omtrent naamgeving e.d.

Certificate Generation Service
Een dienst die certificaten creëert en tekent, gebaseerd op de identiteit en andere door de Registration Authority geverifieerde kenmerken.

Certificate Policy - CP
Een schriftelijk vastgelegde verzameling regels die de toepasbaarheid van een certificaat aangeeft voor een bepaalde gemeenschap en/of toepassingsklasse met gemeenschappelijke beveiligingseisen. Met behulp van een CP kunnen eindgebruikers en vertrouwende partijen bepalen hoeveel vertrouwen zij kunnen stellen in het verband tussen de publieke sleutel en de identiteit van de houder van de publieke sleutel.

Certificate Revocation List – CRL
Een openbaar toegankelijke en te raadplegen lijst (databank) van ingetrokken certificaten, beschikbaar gesteld, ondertekend en onder verantwoordelijkheid vallend van de uitgevende CSP.

Certificate validity period
Zie "Certificaatgeldigheidsduur".

Certificatie
Een brede (zowel technisch als niet-technisch) evaluatie van de beveiligingseigenschappen van een informatiesysteem of, zoals in het kader van de PKI voor de overheid, een managementsysteem. Certificatie wordt uitgevoerd als een onderdeel van een proces, waarbij wordt nagegaan in welke mate een managementsysteem overeenkomt met een vastgestelde verzameling van eisen (ETSI TS 101 456). De regels voor de certificering zijn vastgelegd in een schema: Scheme for Certification of Certification Authorities against ETSI TS 101 456.

Certificatiediensten
Het afgeven, beheren en intrekken van certificaten door certificatiedienstverleners, alsmede andere diensten die samenhangen met het gebruik van elektronische handtekeningen, identiteit en vertrouwelijkheid.

Certificatiedienstverlener
Zie "Certification Service Provider".

Certification Authority – CA
Een organisatorisch verband, welk onderdeel is van een Certificatiedienstverlener of die onder verantwoordelijkheid van de Certificatiedienstverlener handelt en die door één of meer eindgebruikers wordt vertrouwd om Certificaten te maken (genereren), toe te wijzen en in te trekken. Optioneel kan een CA de sleutels voor eindgebruikers aanmaken. Zie ook het plaatje bij "Hiërarchisch model".

Certification Practice Statement – CPS
Een document dat de door een CSP gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de dienstverlening beschrijft. Het CPS beschrijft daarmee op welke wijze de CSP voldoet aan de eisen zoals gesteld in de van toepassing zijnde CP.

Certification Service Provider - CSP (NL: Certificatiedienstverlener)
Een natuurlijke of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent. [Wet EH]

In het kader van de PKI voor de overheid kan de CSP ook diensten verlenen in verband met identiteit en vertrouwelijkheid.
Een CSP heeft als functie het verstrekken en beheren van certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene dragers (bijvoorbeeld smartcards). De CSP heeft tevens de eindverantwoordelijkheid voor het leveren van de certificatiediensten. Daarbij maakt het niet uit of de CSP de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen. Het is bijvoorbeeld niet ondenkbaar dat een CSP de CA-functie en/of de RA-functie uitbesteedt. Zie ook het plaatje bij "Hiërarchisch model".

Certification Service Provider-Certificate Policy – CSP-CP
Een Certificate Policy met betrekking op het certificaat van de CSP.

Cliënt
Zie "Eindgebruiker".

Cliënt-certificaat
Zie "Eindgebruikercertificaat".

Common Criteria – CC
Een verzameling van internationaal geaccepteerde semantische hulpmiddelen en constructies om de beveiligingswensen van klanten en de veiligheidskenmerken van systemen en producten met IT-beveiligingsfuncties te beschrijven. De Common Criteria vormen een hulpmiddel bij de ontwikkeling en aanschaf van dergelijke producten en systemen. Gedurende evaluatie op grond van de Common Criteria wordt een dergelijk product of systeem een TOE genoemd.

Common Data Security Architecture - CDSA
Deze architectuur voorziet in een open, platform onafhankelijk, interoperabel en uitbreidbaar software raamwerk dat bestaat uit API's die zijn ontworpen om computerplatformen veiliger te maken voor applicaties.
CommonName - CN
Een aanduiding van de certificaathouder, in het geval van een persoonsgebonden certificaat bestaande uit: achternaam, voorna[a]m[en] en eventueel voorletters. Ook de certificaatuitgever kan worden aangeduid met een CommonName, in dat geval zal deze meestal bestaan uit een

bedrijfsnaam aangevuld met het van toepassing zijnde domein van de PKI voor de overheid.

Compromittatie
Iedere aantasting van het vertrouwen in het exclusief gebruik van een component door bevoegde personen.
In het kader van de PKI voor de overheid wordt met die component meestal de private sleutel bedoeld. Een sleutel wordt als aangetast beschouwd in geval van:

- ongeautoriseerde toegang of vermeende ongeautoriseerde toegang;
- verloren of vermoedelijk verloren private sleutel of SSCD;
- gestolen of vermoedelijk gestolen private sleutel of SSCD; of
- vernietigde private sleutel of SSCD.

Een compromittatie vormt aanleiding om een certificaat op de Certificate Revocation List te plaatsen.

Cross-certification
Een onderzoek door één of meer Certification Authorities uitgevoerd naar elkaars werkwijze en methoden en een beoordeling van de van toepassing zijnde Certificate Policies en Certification Practice Statements.
Doel van dit proces is om de certificaten uit een andere PKI binnen de "eigen" PKI van een bepaald betrouwbaarheidsniveau te voorzien, zodat het mogelijk wordt elkaars certificaten te accepteren.

Cross-recognition
Een situatie waarbij verschillende PKI's elkaar erkennen zonder daarbij elkaars sleutels te tekenen. Een gevolg van cross-recognition is dat eindgebruikers van de PKI's met elkaar elektronisch kunnen communiceren op een zelfde betrouwbaarheidsniveau.

Cryptografisch profiel
Een verzameling van cryptografische algoritmes en andere voor beveiliging relevante functies, zoals hashfuncties, samen met de parametergrenzen, die worden gebruikt om elektronische handtekeningen te maken of te verifiëren.

Cryptografische module
De verzameling van hardware, software, firmware, of enige combinatie hiervan die cryptografische processen implementeert, inclusief cryptografische algoritmen en die bevat is binnen de cryptografische grenzen van de module.

CSP-certificaat
Een certificaat van een CSP. Met het CSP-certificaat tekent een CSP de certificaten van de onder hem opererende CA's. Binnen de PKI voor de overheid wordt een CSP-certificaat uitgegeven door de Domein-CA onder verantwoordelijkheid van de PA (Policy Authority). Zie ook het plaatje bij "Hiërarchisch model".

CSP-signing
Het ondertekenen van een CSP-certificaat. Binnen de PKI voor de overheid gebeurt dit door middel van de private sleutel van de domein-CA onder verantwoordelijkheid van de PA (Policy Authority). Zie ook het plaatje bij "Hiërarchisch model".

Data Encryption Standard - DES
De standaard symmetrische cryptografie methode van het NIST die een 56-bits sleutel gebruikt. De methode maakt gebruik van een 'block cipher" methode die de tekst in blokjes van 64 bits opsplitst en vervolgens deze bloksgewijs vercijfert. DES is een snel algoritme en wordt algemeen gebruikt. De nieuwe Advanced Encryption Standard (AES) is een opvolger hiervan.

Data To Be Signed - DTBS
Alle elektronische gegevens die moeten worden getekend, met inbegrip van de kenmerken van het document van de ondertekenaar en van de elektronische handtekening.

Decryptie
Het weer leesbaar maken van vercijferde gegevens door gebruik te maken van een cryptografische sleutel. In het geval van symmetrische encryptie is de ontcijfersleutel dezelfde als de vercijfersleutel. In het geval van asymmetrische encryptie zijn de sleutels ongelijk en spreekt men over de sleutels als publieke sleutel en private sleutel.

Digitale handtekening
Zie "Geavanceerde elektronische handtekening".

Digitale identiteit
Zie "Elektronische identiteit".

Directory service
Een dienst van (of met medewerking van) een CSP die de door de Certification Authority uitgegeven certificaten on line beschikbaar en toegankelijk maakt ten behoeve van raadplegende of vertrouwende partijen.

Dissemination Service - DS
Een dienst die certificaten verspreidt onder abonnees en, met toestemming van de abonnees, aan vertrouwende partijen. De dienst verspreidt tevens de Certificate Policies en Certification Practice Statements onder de certificaathouders, abonnees en vertrouwende partijen.

Distinguished Name - DN
De unieke aanduiding van de naam van een certificaathouder, minimaal bestaande uit: land, naam, volgnummer en (in het geval van certificaten in domein Overheid/Bedrijven en Organisatie) organisatienaam.

Domein-certificaat
Een certificaat uitgegeven door de Overheids-CA aan een Domein-CA onder verantwoordelijkheid van de Policy Authority (PA).

Domein-Certificate Policy – Domein-CP
De Certificate Policy met betrekking tot een domein-certificaat.
Domein-Certification Authority – Domein-CA
De Certification Authority die binnen een domein CSP-certificaten aanmaakt. Zie ook het plaatje bij "Hiërarchisch model".

Eindgebruiker (E: End user)

Een natuurlijke of rechtspersoon die een certificaat bezit uitgegeven door een CSP, maar zelf geen certificaten kan uitgeven. Ook wordt soms de term "Gebruiker" gehanteerd.

Eindgebruikercertificaat (E: End user certificate)
Een certificaat uitgegeven door een Certification Service Provider aan een entiteit, zoals een persoon, een computer of een stukje informatie, die zelf geen certificaten kan uitgeven.
Omdat naar de eindgebruiker die een certificaat van een Certification Service Provider ontvangt, vaak wordt verwezen als zijnde de cliënt, wordt dit certificaat ook wel een cliënt-certificaat genoemd. Ook wordt soms de term "Gebruikercertificaat" gehanteerd.

Electronic-signature product (NL: Product voor elektronische handtekeningen)
Software of hardware, of relevante componenten daarvan, die door certificatiedienstverleners kunnen worden gebruikt om diensten op het gebied van elektronische handtekeningen te verlenen of die voor het aanmaken of verifiëren van elektronische handtekeningen kunnen worden gebruikt. [Europese Richtlijn]

Elektronische handtekening (E: Electronic signature)
Een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie. [Wet EH]

In het kader van de PKI voor de overheid:
De elektronische handtekening wordt ingezet om ervoor te zorgen dat elektronische correspondentie en transacties op twee belangrijke punten kunnen wedijveren met de aloude "handtekening op papier". Door het plaatsen van een elektronische handtekening staat vast dat iemand die zegt een document te hebben ondertekend, dat ook daadwerkelijk heeft gedaan. Wie de elektronische handtekening plaatst, geeft aan dat hij/zij de inhoud van het document onderschrijft. Bovendien kan de lezer achteraf ook altijd controleren of de handtekening van de juiste persoon is en of het document onveranderd is gebleven.

Elektronische identiteit
De gegevens in elektronische vorm die worden toegevoegd aan of op logische wijze verbonden met andere elektronische gegevens en fungeren als uniek kenmerk van de identiteit van de eigenaar. Soms wordt de term "Digitale identiteit" gebruikt.

Encryptie
Een proces waarmee gegevens met behulp van een wiskundig algoritme en een cryptografische sleutel worden vercijferd, zodat deze onleesbaar worden voor onbevoegden.
De betrouwbaarheid van de encryptie hangt af van het algoritme, de implementatie daarvan, de lengte van de cryptografische sleutel en de gebruiksdiscipline.
Bij symmetrische encryptie wordt bij het vercijferen en ontcijferen gebruik gemaakt van één en dezelfde, geheime, sleutel.
Bij asymmetrische encryptie wordt gebruik gemaakt van een sleutelpaar. De ene sleutel, de private sleutel, is slechts bekend bij de eindgebruiker van deze sleutel en moet strikt geheim worden gehouden. De andere, de publieke sleutel, wordt verspreid onder communicatiepartners. Wat met

de private sleutel is vercijferd, kan alleen met de bijbehorende publieke sleutel worden ontcijferd, en omgekeerd.

Enhanced Extended Validation Certificates Policy – EVCP+
Een Certificate Policy in aanvulling op de NCP+ policy die moet worden toegepast bij de uitgifte van Extended Validation (EV) SSL certificaten op basis van de EV Guidelines uitgegeven door het CAB Forum. Deze wordt gebruikt in situaties waar het gebruik van een SUD nodig wordt geacht.

Entry
Een afzonderlijk stukje informatie dat is/wordt opgenomen in een register, computer et cetera.

eNIK
De geplande elektronische Nederlandse Identiteitskaart, die naar verwachting PKIoverheid certificaten zal bevatten.

Erkend beroep
In het kader van de PKI voor de overheid wordt als beoefenaar van een erkend beroep alleen beschouwd een natuurlijk persoon die in het bezit is van:

- ofwel een geldig bewijs van inschrijving in een door de betreffende beroepsgroep erkend (beroeps)register waarbij een wettelijk geregeld tuchtrecht van toepassing is;
- ofwel een geldig bewijs (b.v. een vergunning) dat aan de wettelijke eisen voor het uitoefenen van het beroep wordt voldaan.

European Electronic Signature Standardization Initiative - EESSI
Een workshop op Europees niveau met als taak het vormgeven van de concretisering via standaardisatieafspraken van de Europese Richtlijn 1999/93/EG voor elektronische handtekeningen.

European Telecommunications Standards Institute – ETSI
Een organisatie die verantwoordelijk is voor het bepalen van standaarden en normen op telecommunicatiegebied die geldig zijn voor geheel Europa.

Europese Richtlijn
In het kader van PKI wordt hiermee bedoeld het document 1999/93/EG van het Europees parlement en de Raad, d.d.13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (Publicatieblad nr.L013 d.d. 19/01/2000, p.12-20).

Evaluation Assurance Level - EAL
Een pakket bestaande uit betrouwbaarheidscomponenten uit ISO/IEC 15408 Deel 3 die een punt vertegenwoordigen op de betrouwbaarheidsschaal zoals die is gedefinieerd in de Common Criteria.

Extended Normalized Certificate Policy – NCP+
Een Certificate Policy voor niet-gekwalificeerde certificaten die hetzelfde kwaliteitsniveau geeft als voor gekwalificeerde certificaten geldt (in de QCP), maar buiten de werking van de Europese Richtlijn. Deze wordt gebruikt in situaties waar het gebruik van een SUD nodig wordt geacht.

Extended Validation SSL certificaten
EV SSL certificaten worden uitgegeven conform de Extended Validation richtlijn waarin strenge eisen worden gesteld aan de controle van de

organisatie die het SSL certificaat aanvraagt en het domein waarvoor het certificaat wordt aangevraagd. Één van de belangrijkste eigenschappen van een Extended Validation SSL certificaat is dat deze de adresbalk van bijvoorbeeld Internet Explorer (versie 7 en verder) groen laat kleuren.

Exclusiviteit
Zie "Vertrouwelijkheid".FINREAD
Een open standaard voor smartcardlezers die veilige authenticatie op het internet mogelijk maakt. Deze standaard is een resultaat van een Europees initiatief vanuit een aantal financiële instellingen en is gericht op het kunnen uitvoeren van elektronische bancaire transacties. Binnen de FINREAD (voluit: FINancial READer) specificaties worden de cryptografische processen door de kaartlezer afgehandeld en niet door de smartcard.

Fabrikant
In het kader van de PKI voor de overheid is een Fabrikant een in Nederland erkende organisatie, die aantoonbaar conformeert aan het Normenkader voor het produceren en in Nederland verspreiden van een specifieke soort Autonome Apparaten en daarvoor dan ook is geautoriseerd door de Kadersteller.

Federal Information Processing Standard – FIPS
Een officiële standaard voor de Verenigde Staten en uitgegeven door de NIST. In het kader van PKI zijn vooral FIPS 140 ("Security Requirements for Cryptographic Modules") en FIPS 186-2 ("Digital Signature Standard") van belang.

Fully Qualified Domain Name (FQDN)
Een Fully Qualified Domain Name (FQDN) volgens de definitie van PKIoverheid, is een in het Internet Domain Name System (DNS) geregistreerde volledige naam waarmee een server op het Internet uniek is te identificeren en te adresseren. Met die definitie omvat een FQDN alle DNS nodes, tot en met de naam van het desbetreffende Top Level Domein (TLD) en is een FQDN in het Internet DNS geregistreerd onder een DNS Resource Record (RR) van het type “IN A” en/of “IN AAAA” en/of “IN CNAME”.

Voorbeelden van FQDN’s zijn:
- www.logius.nl
- webmail.logius.nl
- local.logius.nl
- server1.local.logius.nl
- logius.nl (mits geregistreerd onder een DNS RR van het type “IN A” en/of “IN AAAA” en/of “IN CNAME”)

Voorbeelden van non-FQDN’s (en dus niet toegestaan binnen PKIoverheid) zijn:
- www
- logius.nl (mits NIET geregistreerd onder een DNS RR van het type “IN A” en/of “IN AAAA” en/of “IN CNAME”)
- server1.webmail
- server1.local
- server1.

Geavanceerde elektronische handtekening (E: advanced electronic signature)
Een elektronische handtekening die voldoet aan de volgende eisen:

A. *Zij is op unieke wijze aan de ondertekenaar verbonden;*
B. *Zij maakt het mogelijk de ondertekenaar te identificeren;*
C. *Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;*
D. *Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;*

[Europese Richtlijn]

In – met name gedateerde – literatuur wordt soms de term "Digitale handtekening" gebruikt. Een geavanceerde elektronische handtekening is, in tegenstelling tot een gekwalificeerde elektronische handtekening, niet onder alle omstandigheden een rechtsgeldige handtekening.

Gebruiker
Zie "Eindgebruiker".

Gebruikercertificaat
Zie "Eindgebruikercertificaat".

Gegevens voor het aanmaken van elektronische handtekeningen
Zie "Signature creation data".

Gegevens voor het verifiëren van een elektronische handtekening
Zie "Signature verification data".

Geheime sleutel
Een cryptografische sleutel die wordt gebruikt bij een symmetrisch cryptografisch algoritme. In de asymmetrische cryptografie – zoals onder andere gebruikt bij de PKI voor de overheid – wordt niet gesproken over geheime sleutels.

Gekwalificeerd certificaat (E: Qualified certificate)
Een certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid van de Telecommunicatiewet, en is afgegeven door een certificatiedienstverlener die voldoet aan de eisen, gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet. [Wet EH]

In het kader van de wet EH wordt alleen het handtekeningcertificaat beschouwd. In het kader van de PKI voor de overheid worden echter nog twee andere typen certificaten behandeld. Alleen het handtekeningcertificaat wordt hierbij beschouwd als een gekwalificeerd certificaat. Het vertrouwelijkheidcertificaat en het authenticiteitcertificaat zijn geen gekwalificeerde certificaten, maar bezitten binnen de PKI voor de overheid wel hetzelfde betrouwbaarheidsniveau.

Gekwalificeerde elektronische handtekening (E: Qualified electronic signature)
Een elektronische handtekening die voldoet aan de volgende eisen:

A. *Zij is op unieke wijze aan de ondertekenaar verbonden;*
B. *Zij maakt het mogelijk de ondertekenaar te identificeren;*
C. *Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;*

D. Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
E. Zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet; en
F. Zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel vv Telecommunicatiewet.

[Wet EH]
Toelichting:
Met de wet wordt beoogd de gekwalificeerde elektronische handtekening rechtsgeldig te maken door haar werking gelijk te stellen aan die van de handgeschreven handtekening.
In de wet staat letterlijk dat als een elektronische handtekening aan a) tot en met f) voldoet, de daarbij gebruikte "methode wordt vermoed voldoende betrouwbaar te zijn". Er wordt echter geen naam aan dit type van handtekeningen gegeven. In de ETSI-norm TS 101 456 wordt wel de naam "Qualified electronic signature" gegeven aan de elektronische handtekening die aan a) tot en met f) voldoet. De hierboven gekozen benaming is dus voor de hand liggend en vult de omissie in de wet op.

Geldigheidsgegevens
Zie "Validity Data".

Glue
Software die de brug vormt tussen de applicatieve functies, zoals deze op de clients en servers draaien en de cryptografische functies, zoals deze door smartcard en kaartlezer worden uitgevoerd.

Generiek TopLevelDomein (gTLD)
De gTLD is een generiek topleveldomein (generic Top Level Domain), een domeinnaam extensie die niet aan een bepaald land toebehoort en die in principe door iedereen waar ook ter wereld geregistreerd kan worden. Enkele voorbeelden van gTLD's zijn .com, .edu, .gov, .mil en .org.

Handtekeningcertificaat
Een certificaat dat wordt gebruikt bij het plaatsen van een elektronische handtekening.

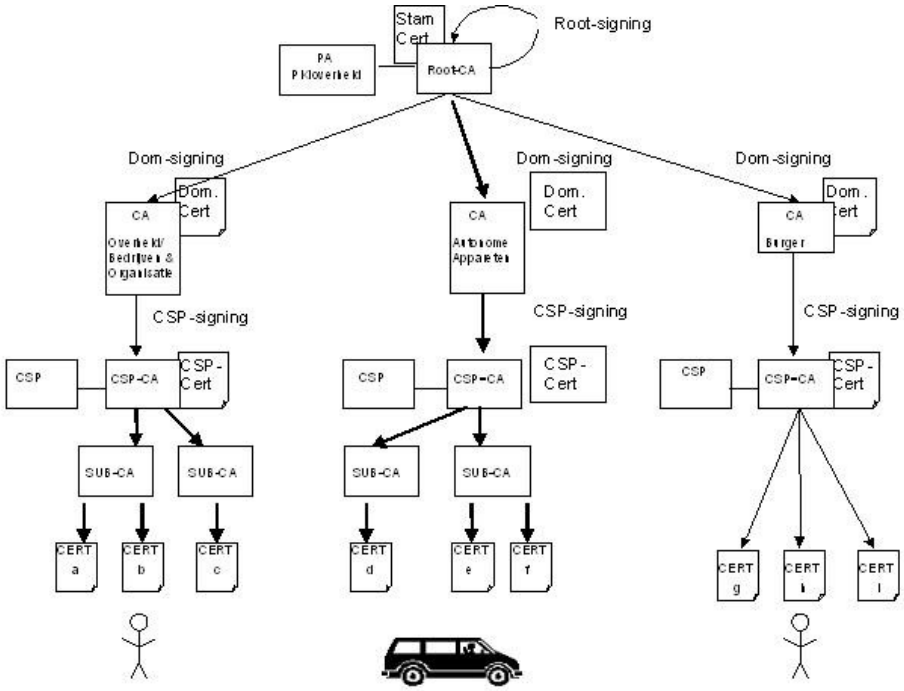
Hardware Security Module - HSM
De randapparatuur die wordt gebruikt aan de serverkant om cryptografische processen te versnellen. Met name dient hierbij gedacht te worden aan het aanmaken van sleutels.

Hashfunctie
Een functie die een bericht van willekeurige lengte omzet in een reeks met een vaste lengte en voldoet aan de volgende voorwaarden:
- Het is praktisch onuitvoerbaar om voor een gegeven uitvoer een invoer te vinden die deze uitvoer als resultaat heeft ("one-way");
- Het is praktisch onuitvoerbaar om voor een gegeven invoer een tweede invoer te vinden die dezelfde uitvoer als resultaat heeft ("zwak collision-free");
- Het is praktisch onuitvoerbaar om twee willekeurige berichten te vinden die dezelfde uitvoer als resultaat hebben ("sterk collision-free").

Hashwaarde

Het resultaat (uitvoer) van een hashfunctie. De hashwaarde wordt ook wel "message digest" genoemd.

Hiërarchisch model
De PKI voor de overheid gaat uit van een hiërarchisch model. Dat betekent dat het vertrouwen in een keten doorgegeven wordt. Een eindgebruiker kan daarmee alle Certification Authorities vertrouwen die onder dezelfde stam-CA vallen.



Identificatie
Het vaststellen van de identiteit van een persoon (of zaak).

Identiteit en Authenticiteit Certificaat
Zie "Authenticiteitcertificaat".

Identiteitcertificaat
Zie "Authenticiteitcertificaat".

Incident
Een gebeurtenis die geen onderdeel uitmaakt van de standaardwerking van een dienst en die een onderbreking van, of een reductie in, de kwaliteit van die dienst veroorzaakt of kan veroorzaken.

Indirecte fysieke verschijning
Een begrip dat wordt gebruikt wanneer de identiteitcontrole van een persoon niet geschiedt met behulp van persoonlijke aanwezigheid van die persoon, maar in plaats daarvan met behulp van middelen waarmee dezelfde zekerheid kan worden verkregen als bij persoonlijke aanwezigheid.

Information Asset
Een (benoemd) onderdeel van de informatie binnen een organisatie die benodigd is voor de continuïteit van de werkprocessen (primair én secundair).

Integriteit
De zekerheid dat gegevens volledig zijn en niet zijn gewijzigd, ongeacht of dat opzettelijk, niet opzettelijk door menselijk toedoen of anderszins is gebeurd.

Internet Engineering Task Force – IETF
Een internationale organisatie die zich in wil zetten voor de ontwikkeling van de internet architectuur vanuit technisch-wetenschappelijk oogpunt.

Interoperabiliteit
Het vermogen te bewerkstelligen dat verschillende (geautomatiseerde) systemen technisch met elkaar kunnen werken.

Kadersteller
In het kader van de PKI voor de overheid is een Kadersteller een overheidsinstantie die:

- voor een bepaalde kerntaak de behoefte heeft aan – van buiten haar directe invloedssfeer afkomstige – (meet)gegevens;
- voor het waarborgen van de integriteit en authenticiteit van die (meet)gegevens gebruik wenst te maken van autonoom handelende apparaten van een bepaalde soort;
- voor het waarborgen van de betrouwbaarheid van exemplaren van die apparaatsoort:
    - een normenkader voor de productie, activering, operatie, onderhoud, inname en gebruik opstelt en in wet- en regelgeving vastlegt;
    - op basis van dat normenkader organisaties autoriseert voor:
        - het produceren en verspreiden van apparaten van betreffende soort;
        - het koppelen van certificaten aan apparaten van betreffende soort;
        - het vervangen van certificaten op apparaten van betreffende soort;
        - het intrekken van certificaten van apparaten van betreffende soort.

Key-backup
Het maken van een kopie van een private sleutel bij uitgifte. Veelal is dit bedoeld om deze kopie te overhandigen aan een organisatie die er door middel van key-escrow gebruik van kan maken.

Key-escrow
Een methode van opslag voor (een kopie van) een private sleutel, waarbij deze bij een vertrouwde derde partij (een zogeheten "Key Escrow Agency" - KEA) in bewaring wordt gegeven. Indien noodzakelijk kunnen daartoe geautoriseerde betrokkenen toegang krijgen tot de sleutel.

Key-recovery
De techniek waarbij de sleutel die nodig is om een vercijferd bericht te ontcijferen per bericht te herleiden is door een derde partij.

Land code TopLevelDomein (ccTLD)
De ccTLD (country code Top Level Domain) dit is de domeinnaam extensie voor een land of onafhankelijk grondgebied. Een ccTLD bestaat uit de 2-letterige landcode die volgens de ISO 3166-1 norm is vastgelegd. B.v. .nl, .be en .de.

Leveranciersverklaring
Verklaring van een leverancier waarin hij onder zijn uitsluitende verantwoordelijkheid beweert, dat een product, proces of dienst in overeenstemming is met een gespecificeerde standaard of ander normatief document.

Lightweight Certificate Policy – LCP
Een Certificate Policy die gebruikt wordt voor niet-gekwalificeerde certificaten in situaties waar een risico-analyse niet de additionele kosten van zwaardere vereisten van de NCP (zoals fysieke verschijning bij het aanvraagproces) rechtvaardigt.

Lightweight Directory Access Protocol - LDAP
Een open protocol dat applicaties in staat stelt om informatie uit directories te verkrijgen, zoals bijvoorbeeld e-mail adressen en sleutels.

Lokale Registration Authority - LRA
De organisatie-eenheid of functie, aan wie de uitvoering van de taak van Registration Authority is opgedragen, en die fysiek de identificatie gegevens van een aanvrager verzamelt, controleert, registreert en doorstuurt ten behoeve van de certificaatuitgifte.

Message Digest - MD
Zie "Hashwaarde".

MD5-algoritme
Een veel gebruikt algoritme voor het creëren van een cryptografische hashwaarde van een bericht. De MD5-waarde van een certificaat is uniek voor dat certificaat, en wordt vaak gebruikt om een certificaat te identificeren.

Middel voor het aanmaken van elektronische handtekeningen
Zie "Signature Creation Device".

Middel voor het verifiëren van een elektronische handtekening
Zie "Signature Verification Device".

Multi-factor authenticatie
Bij deze vorm van authenticatie worden minimaal twee authenticatie technieken gelijktijdig toegepast.

Niet-gekwalificeerd certificaat
Een certificaat dat niet voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid van de Telecommunicatiewet, en/of niet is afgegeven door een CSP die voldoet aan de eisen, gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet en/of niet tot toepassing van de geavanceerde elektronische handtekening strekt.

Toelichting: In het kader van de PKI voor de overheid zijn het Authenticiteitcertificaat en het vertrouwelijkheidcertificaat formeel niet-gekwalificeerde certificaten, maar inhoudelijk voldoen ze wel aan dezelfde eisen en hebben ze daardoor hetzelfde betrouwbaarheidsniveau.

Non-Qualified Certificate – NQC
Zie "Niet-gekwalificeerd certificaat".

Non-repudiation (NL: Onloochenbaarheid, Onweerlegbaarheid)
De eigenschap van een bericht om aan te tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten.
Binnen de PKI voor de overheid wordt non-repudiation (van de inhoud van een bericht) bewezen door middel van het handtekeningcertificaat.

Normalized Certificate Policy – NCP
Een Certificate Policy voor niet-gekwalificeerde certificaten die hetzelfde kwaliteitsniveau geeft als voor gekwalificeerde certificaten geldt (in de QCP), maar buiten de werking van de Europese Richtlijn 1999/93/EG en zonder dat het gebruik van een secure user device vereist is.

Notified body (NL: Aangemelde instantie)
Een instantie die is voorgedragen door de overheid van een EU-lidstaat en hiervan melding heeft ontvangen door de EU, om taken uit te voeren met betrekking tot de procedures voor conformiteittests waarnaar verwezen wordt in de betreffende "Nieuwe aanpak richtlijnen" van de EU daar waar een derde partij vereist wordt.
In het kader van elektronische handtekeningen wordt een dergelijke instantie ook wel "designated body" genoemd en wordt als zodanig aangewezen om te bepalen of een product voldoet aan de eisen voor SSCD's op grond van de Europese Richtlijn 1999/93/EG.

Object Identifier - OID
Een rij van getallen gescheiden door punten die op unieke wijze en permanent een object aanduidt. Binnen de PKI voor de overheid worden OID's toegekend aan alle CP's en aan alle CA's.

Ondertekenaar (E: Signatory)
(Voor de toepassing van de Telecommunicatiewet) Degene die een middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel uu Telecommunicatiewet gebruikt. [Wet EH]
In het kader van de PKI voor de overheid wordt onder de certificaathouder van het handtekeningcertificaat de ondertekenaar verstaan en wordt de term 'ondertekenaar' zelf niet gehanteerd.

Online Certificate Status Protocol - OCSP
Een methode om de geldigheid van certificaten on line (en real-time) te controleren. Deze methode kan worden gebruikt als alternatief voor het raadplegen van de Certificate Revocation List.

Onloochenbaarheid
Zie "non-repudiation".

Onweerlegbaarheid
Zie "non-repudiation".

Open Card Framework - OCF
Door gebruik te maken van Java en de Java Virtual Machine (VM) kan een open architectuur worden gerealiseerd op basis waarvan compatibele

API's kunnen worden opgeleverd. Het is derhalve wenselijk dat de smartcardreader het gebruik van Java en Java VM ondersteunt.

Openbare sleutel
Zie "Publieke sleutel".

Organisatiegebonden certificaten
Er zijn twee verschillende soorten organisatiegebonden certificaten:
1. voor personen;
2. voor services.

Ad. 1
Bij organisatiegebonden certificaten voor personen is de certificaathouder onderdeel van een organisatorische entiteit. De certificaathouder heeft de bevoegdheid een bepaalde transactie namens die organisatiorische entiteit te doen.

Ad. 2
Bij organisatiegebonden certificaten voor services is de certificaathouder:
- een apparaat of een systeem (een niet-natuurlijke persoon), bediend door of namens een organisatorische entiteit; of
- een functie van een organisatorische entiteit.

Overheid
Binnen de context van PKIoverheid wordt/worden als overheid c.q. als overheidsorganisaties beschouwd:
- het geheel van het Rijk, de provincies, de gemeenten, de samenwerkingsverbanden op grond van de Wet Gemeenschappelijke Regelingen en de waterschappen;
- uitvoerende organisaties en diensten zoals inspecties, baten en lastendiensten en politiediensten;
- rechterlijke macht;
- zelfstandige bestuursorganen zoals vermeldt in het ZBO-register[1]

Overheid/Bedrijven en Organisatie
Binnen de PKI voor de overheid bestaan de domeinen Overheid/Bedrijven en Organisatie uit alle organisaties binnen overheid en bedrijfsleven.

Personal Unblocking Key - PUK
De deblokkeringcode voor cryptografische modules.

Personalisatie
Een proces waarbij blanco kaarten worden voorzien van persoonsgebonden gegevens (foto en/of NAW-gegevens) en/of persoonsgebonden sleutelmateriaal.
Het is waarschijnlijk dat in het kader van de PKI voor de overheid de personalisatie door twee verschillende aanbieders wordt uitgevoerd, waarbij de één het sleutelmateriaal plaatst in aanwezigheid van de eindgebruiker en de ander de kaart bedrukt met de foto en de relevante persoonsgebonden gegevens.

Persoonsgebonden certificaten
De certificaathouder zal in het geval van persoonsgebonden certificaten een natuurlijke persoon zijn. De certificaathouder is ofwel onderdeel van een organisatorische entiteit waarvoor een abonnee de contracterende

1 http://almanak.zboregister.overheid.nl/sites/min_bzk2/index.php

partij is (organisatiegebonden certificaathouder), ofwel de beoefenaar van een erkend beroep en in die hoedanigheid zelf een abonnee en daarmee de contracterende partij (beroepsgebonden certificaathouder) ofwel een burger en in die hoedanigheid zelf een abonnee en daarmee de contracterende partij.

PKI voor de overheid
De gehele infrastructuur die door de PA PKIoverheid wordt beheerd.

PKI-enabled applicatie
Een applicatie die in staat is gebruik te maken van PKI-functies, zoals het plaatsen van een elektronische handtekening.

Plug and Play - PnP
Een standaard voor automatische configuratie of installatie van hardware middelen.

Policy Authority – PA
Een autoriteit die de regels vaststelt voor het onder haar zeggenschap berustende deel van de hiërarchie van een PKI.

Policy Authority PKIoverheid – PA PKIoverheid
De Policy Authority (PA) voor de hiërarchie van de PKI voor de overheid. De PA ondersteunt de minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid. De dienstverlening van de PA is onder te verdelen in het beheren van de bovenste lagen van de infrastructuur, het toelaten van CSP's tot de infrastructuur en het houden van toezicht op de betrouwbaarheid van de PKI voor de overheid. Zie ook het plaatje bij "Hiërarchisch model".

Prepersonalisatie
Een proces waarbij witte kaarten worden voorzien van generiek materiaal (zoals bedrukking of generieke sleutels), maar nog niet van persoonsgebonden gegevens of persoonsgebonden sleutelmateriaal.

Privaat IP adres
Een Internet Protocol adres (IP adres) is een identificatienummer toegewezen aan elk apparaat (b.v. computer, printer) dat deelneemt aan een computernetwerk dat het Internet Protocol (TCP/IP) gebruikt voor de communicatie.

Private IP adressen zijn niet routeerbaar op het internet en zijn gereserveerd voor particuliere netwerken. De binnen IPv4 voor privégebruik vrijgehouden c.q. gereserveerde IP adressenreeks is (zie RFC 1918):
- 10.0.0.0 – 10.255.255.255;
- 172.16.0.0 – 172.31.255.255;
- 192.168.0.0 – 192.168.255.255;

Daarnaast is de reeks van 169.254.0.0 -169.254.255.255 gereserveerd voor Automatic Private IP Addressing (APIPA). Deze IP adressen mogen niet worden gebruikt op het internet.

De binnen IPv6 voor privégebruik vrijgehouden c.q. gereserveerde IP adressen reeks is (zie RFC 4193):
- fc00::/7

Daarnaast is de reeks van fe80::/10 gereserveerd voor Automatic Private IP Addressing (APIPA). Deze IP adressen mogen niet worden gebruikt op het internet.

Private key
Zie "Private sleutel".

Private sleutel (E: Private key)
De sleutel van een asymmetrisch sleutelpaar die alleen bekend dient te zijn bij de houder ervan en strikt geheim moet worden gehouden.
In het kader van de PKI voor de overheid wordt de private sleutel door de bezitter gebruikt om zich elektronisch te identificeren, zijn elektronische handtekening te zetten of om een vercijferd bericht te ontcijferen.
Ook wordt vaak de term "privé sleutel" (Onder andere in de Europese Richtlijn) gebruikt. In de Wet EH wordt echter "private sleutel" gebruikt. Beide zijn bedoeld als vertaling van de Engelstalige term "private key".

Privé sleutel
Zie "Private sleutel".

Proceseigenaar
Een rol in het procesmanagement die de doelmaatregelen definieert, de consistente implementatie van het proces in hun verantwoordelijkheidsgebied verzekert, resources om aan procesverbetering te werken aanvraagt en zeker stelt, procesveranderingen beoordeelt en procesveranderingen en verbeteringen aan procesgebruikers communiceert.

Product voor elektronische handtekeningen
Zie "Electronic-signature product".

Protection Profile – PP
Een verzameling van beveiligingseisen, onafhankelijk van de implementatie, voor een categorie van TOE's die tegemoetkomen aan specifieke klantwensen.

Public key
Zie "Publieke sleutel".

Public key cryptografie
Het systeem waarbij een mechanisme van publieke sleutels en private sleutels wordt gebruikt. Dit houdt in dat er twee sleutels worden gebruikt. Eén sleutel wordt geheim gehouden (de private sleutel) en de andere sleutel mag publiekelijk worden verspreid (de publieke sleutel). Alles wat met de publieke sleutel vercijferd wordt is alleen met de private sleutel te ontcijferen en andersom. Het is een vorm van asymmetrische encryptie.

Public Key Cryptography Standard - PKCS
Een standaard op het gebied van public key cryptografie, ontwikkeld door RSA-laboratories. In het kader van de PKI voor de overheid zijn vooral PKCS#7 (Cryptographic Message Syntax Standard), PKCS#10 (Certification Request Syntax Specification), PKCS#11 (Cryptographic Token Interface Standard), PKCS#12 (Personal Information Exchange Syntax Standard) en PKCS#15 (Cryptographic Token Information Format Standard) van belang.

Public Key Infrastructure - PKI
Een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op public key cryptografie. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.

Publieke sleutel (E: Public key)
De sleutel van een asymmetrisch sleutelpaar die publiekelijk kan worden bekendgemaakt.
De publieke sleutel wordt gebruikt voor de controle van de identiteit van de eigenaar van het asymmetrisch sleutelpaar, voor de controle van de elektronische handtekening van de eigenaar van het asymmetrisch sleutelpaar en voor het vercijferen van informatie voor een derde.
Ook wordt de term "openbare sleutel" (Onder andere in de Europese Richtlijn) gebruikt. In de wet EH wordt echter "publieke sleutel" gebruikt. Beide zijn bedoeld als vertaling van de Engelstalige term "public key".

Publiek IP adres
Publieke IP adressen zijn wereldwijd uniek en kunnen routeerbaar, zichtbaar en benaderbaar zijn vanaf het internet.

Qualified Certificate – QC
Zie "Gekwalificeerd certificaat".

Qualified Certificate Policy – QCP
Een Certificate Policy die een uitwerking van de vereisten bevat die zijn omschreven in artikel 18.15, eerste en tweede lid van de Telecommunicatiewet.

Qualified electronic signature
Zie "Gekwalificeerde elektronische handtekening".

Regeling elektronische handtekeningen
De regeling die gelijktijdig met de wet EH van kracht is geworden. De regeling geeft nadere regels met betrekking tot elektronische handtekeningen, zoals technische en organisatorische uitwerking van gestelde eisen. Nr. WJZ/03/02263.

Registerhouder
Een instantie die gegevens verzamelt en vastlegt in een register. De registerhouder is hierbij verantwoordelijk voor de definitie en specificatie van de registratie en de inrichting van de opslag- en communicatiefaciliteiten om hergebruik mogelijk te maken. De registerhouder moet voldoen aan een aantal minimumeisen, maar heeft ook de vrijheid om zelf bepaalde keuzes te maken op dit gebied. Veelal registreert een registerhouder ook andere gegevens over de objecten waarvan deze zelf de identiteit heeft vastgesteld.

Registration Authority – RA
Een entiteit binnen de verantwoordelijkheid van de CSP. Een Registration Authority zorgt voor de verwerking van certificaataanvragen en alle daarbij behorende taken waarbij de verificatie van de identiteit van de certificaathouder de belangrijkste is. De RA heeft een duidelijke relatie met een of meerdere Certification Authorities: De RA geeft – na de verificatie - opdracht aan de Certification Authorities voor de productie

van certificaten. Een RA kan tegelijkertijd voor meerdere Certification Authorities functioneren.

Registration service
Een dienst die de identiteit en, indien van toepassing, overige specifieke kenmerken van een abonnee verifieert. De resultaten hiervan worden doorgegeven aan de Certificate Generation Service.

Relying Party - RP
Zie "Vertrouwende partij".

Request for Comments - RFC
Een voorstel voor een standaard afkomstig van de IETF. Hoewel een RFC niet de formele status van een standaard heeft, worden in praktijk de RFC's normaliter gevolgd.

Reseller
Een persoon of entiteit die toestemming heeft gekregen van de CSP om namens de CSP, PKI certificaten te verkopen aan abonnees.

Revocation management service
Een dienst die verzoeken, die te maken hebben met intrekking van certificaten, behandelt en rapporteert, om zo de te nemen maatregelen te bepalen. De resultaten worden verspreid door middel van de Revocation Status Service.

Revocation service
Een dienst van een CSP waarbij deze certificaten intrekt bij beëindiging van de overeenkomst, constatering van fouten in het certificaat of bij compromittatie van de private sleutel die hoort bij de in het certificaat opgenomen publieke sleutel. De ingetrokken certificaten worden opgenomen in de Certificate Revocation List.

Revocation status information
Informatie die nodig is om op een zeker moment de geldigheid van een certificaat te kunnen aantonen. Deze informatie kan beschikbaar gesteld worden bijvoorbeeld door middel van een Online Certificate Status Protocol of Certification Revocation Lists.

Revocation status service
Een dienst die certificaatinformatie over de revocatiestatus levert aan vertrouwende partijen. Deze dienst kan een real-time dienst zijn, maar kan ook zijn gebaseerd op revocatiestatus informatie die wordt geüpdate op regelmatige intervallen.

Race Integrity Primitives Evaluation Message Digest - RIPEMD
Een eenwegs Hashfunctie. Het aantal bits van de hieruit volgende hashwaarde wordt er meestal direct achter weergegeven. Zo levert de veel gebruikte RIPEMD-160 een 160-bits uitvoer op.

Rivest-Shamir-Adleman algoritme – RSA-algoritme
Een cryptografische methode die gebruik maakt van een tweeledige sleutel. De private sleutel wordt bewaard door de eigenaar; de publieke sleutel wordt gepubliceerd. Data wordt vercijferd met de publieke sleutel van de ontvanger en kan alleen ontcijferd worden met de private sleutel van de ontvanger. Het RSA-algoritme is rekenintensief, waardoor het vaak

wordt gebruikt om een digitale envelop te maken, die een met RSA vercijferde DES sleutel bevat en met DES vercijferde data.

Root (NL: Stam)
Het centrale gedeelte van een (PKI-) hiërarchie waaraan de gehele hiërarchie en haar betrouwbaarheidsniveau is opgehangen.

Root certificate
Zie "Stamcertificaat".

Root Certification Authority – Root-CA (NL: Stam-Certification Authority – Stam-CA)
Een Certification Authority die het centrum van het gemeenschappelijke vertrouwen in een PKI-hiërarchie is. Het CA-certificaat van de Root-CA ("stamcertificaat") is self-signed, waardoor het niet mogelijk is de bron van de handtekening op dit certificaat te authenticeren, alleen de integriteit van de inhoud van het certificaat. De Root-CA wordt echter vertrouwd omdat iemand anders dat verteld of omdat men de CP en eventuele andere documenten van de Root-CA heeft gelezen en deze bevredigend vindt.

Root-signing
Het ondertekenen van het certificaat van de Root-CA – het stamcertificaat – door de Root-CA zelf. Zie ook het plaatje bij "Hiërarchisch model".

Secure Hash Algorithm - SHA
Een bepaald algoritme dat een concrete invulling geeft voor een Hashfunctie. Het nog veel gebruikte SHA-1 is ontwikkeld door de Amerikaanse overheid en maakt een Message Digest van 160 bits aan. De Advanced Encryption Standard en SHA-2 zijn opvolgers hiervan.

Secure Multi-Purpose Internet Mail Extensions – S/MIME
Een veilige methode voor het versturen van e-mail. De e-mail clients van zowel Netscape als Microsoft ondersteunen S/MIME. MIME, zoals beschreven in RFC 1521, omschrijft hoe een elektronisch bericht moet worden georganiseerd. S/MIME beschrijft hoe encryptie informatie en een certificaat toegevoegd kunnen worden als onderdeel van de tekst van het bericht. S/MIME volgt de syntax gegeven in het PKCS#7 document. S/MIME veronderstelt een PKI voor het elektronisch ondertekenen van e-mail berichten en voor het ondersteunen van encryptie van berichten en attachments.

Secure Signature Creation Device - SSCD (NL: Veilig middel voor het aanmaken van elektronische handtekeningen)
Een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid van de Telecommunicatiewet. [Wet EH]

Binnen de PKI voor de overheid is in domein Burger gekozen voor de smartcard als SSCD. In domein Overheid/Bedrijven en Organisatie kunnen zowel smartcards als USB-tokens worden gebruikt, mits deze aan de gestelde eisen voldoen.

Secure Sockets Layer - SSL
Een protocol gecreëerd door Netscape voor het beheer van de veiligheid van bericht verzendingen in een netwerk en de toegang tot web servers.

Het woord sockets verwijst hierbij naar de methode om data heen en weer tussen een client en een server programma te sturen in een netwerk of tussen programmalagen in dezelfde computer.

Secure User Device – SUD (NL: Veilig gebruikersmiddel)
Een middel dat de private sleutel(s) van de gebruiker bevat, deze sleutel(s) tegen compromittatie beschermt en elektronische ondertekening, authenticatie of ontcijfering uitvoert namens de gebruiker.

Security Function - SF
Eén of meerdere delen van een TOE waarop dient te worden vertrouwd om een nauw verwante deelverzameling van regels van de Certificate Policy ten aanzien van de TOE op te leggen.

Security policy
De verzameling van regels, neergelegd door de beveiligingsautoriteit, die het gebruik van en de maatregelen ten aanzien van beveiligingsdiensten en faciliteiten regelen.

Self-signed certificaat
Een certificaat voor een Certification Authority, getekend door die Certification Authority zelf. Dit kan alleen bij het stamcertificaat van een hiërarchie.

Services certificaat
Een certificaat waarmee een functie of apparaat, bijvoorbeeld een server, wordt gekoppeld aan een rechtspersoon of andere organisatie. In het geval van een server wordt het certificaat gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server die behoort bij de organisatorische entiteit die als abonnee wordt genoemd in het betreffende certificaat. Een services certificaat is geen gekwalificeerd certificaat.

Sessiesleutel
Een symmetrische sleutel die één keer wordt gebruikt voor een berichtenuitwisseling of een telefoongesprek (een sessie). Na afloop van de berichtenuitwisseling of het telefoongesprek wordt de sleutel weggegooid.

Signatory
Zie "Ondertekenaar".

Signature creation data (NL: Gegevens voor het aanmaken van elektronische handtekeningen)
Unieke gegevens, zoals codes of cryptografische private sleutels, die door de ondertekenaar worden gebruikt om een elektronische handtekening te maken. [Europese Richtlijn]

Signature Creation Device - SCD (NL: Middel voor het aanmaken van elektronische handtekeningen)
Geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het aanmaken van elektronische handtekeningen te implementeren. [Wet EH]

Signature verification data (NL: Gegevens voor het verifiëren van een elektronische handtekening)
Gegevens, zoals codes of cryptografische publieke sleutels, die worden gebruikt voor het verifiëren van een elektronische handtekening.
[Europese Richtlijn]

Signature Verification Device – SVD (NL: Middel voor het verifiëren van een elektronische handtekening)
Geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het verifiëren van een elektronische handtekening te implementeren.
[Europese Richtlijn]

Signing key (NL: Tekensleutel)
De private sleutel die wordt gebruikt om een elektronische handtekening te zetten. Er kan onderscheid worden gemaakt tussen een signing key van een Certification Authority en een signing key van een eindgebruiker. Met de signing key van de eindgebruiker plaatst deze diens elektronische handtekening. Met de signing key van de Certification Authority worden onder andere de uitgegeven certificaten getekend en wordt de Certificate Revocation List getekend.

Single Sign-On - SSO
Een procedure waarbij slechts één authenticatie per sessie nodig is, waardoor het niet nodig is dat eindgebruikers zich binnen een sessie voor meerdere applicaties moeten authenticeren.

Sleutelbeheerdiensten
Het genereren, opslaan, verstrekken of vernietigen van cryptografisch sleutelmateriaal dat gebruikt wordt voor het aanmaken of verifiëren van elektronische handtekeningen. [Besluit elektronische handtekeningen]
Toelichting: Sleutelbeheerdiensten kunnen door een CSP worden uitgevoerd of (deels) door de certificaathouder zelf. Het begrip 'sleutelbeheerdiensten' wordt niet afzonderlijk gehanteerd in de context van de PKI voor de overheid.

Sleutelpaar
In een asymmetrisch cryptografische systeem is dit een private sleutel en zijn wiskundig verbonden publieke sleutel. Deze hebben de eigenschap dat met behulp van de publieke sleutel een elektronische handtekening kan worden geverifieerd die met een private sleutel is gemaakt. In het geval van encryptie betekent deze eigenschap dat informatie die met de publieke sleutel is vercijferd met behulp van de private sleutel kan worden ontcijferd (of andersom).

Smartcard
Een plastic kaart ter grootte van een creditcard die in een chip elektronica bevat, inclusief een microprocessor, geheugenruimte en een voedingsbron. De kaarten kunnen worden gebruikt om informatie op te slaan en zijn makkelijk mee te nemen. In de toekomst zal de elektronische Nederlandse Identiteitskaart (eNIK) een smartcard zijn.
Stam-Certification Authority – Stam-CA (E: Root Certification Authority - Root-CA)
Zie "Root Certification Authority".

Stamcertificaat (E: Root certificate)

Het certificaat van de Root-CA. Dit is het certificaat behorend bij de plek waar het vertrouwen in alle binnen de PKI voor de overheid uitgegeven certificaten zijn oorsprong vindt. Dit certificaat wordt door de CA van de houder (binnen de PKI voor de overheid is dat de PA PKIoverheid) zelf ondertekend. Alle onderliggende certificaten worden uitgegeven door de houder van het stamcertificaat. Zie ook het plaatje bij "Hiërarchisch model".

Strength of Function - SOF
Een kwalificatie van een TOE beveiligingsfunctie die het minimum aan maatregelen uitdrukt die nodig worden geacht om het beveiligingsgedrag van die functie uit te schakelen door een directe aanval op haar onderliggende beveiligingsmechanismen uit te voeren.

Subject Device Provision Service
Een dienstverlening waarvan sprake is indien de CSP het genereren verzorgt van private en publieke sleutels op SSCD's. In dat geval bereidt de Subject Device Provision Service de levering van SSCD's voor en voert die uit en levert tevens de private sleutels aan de eindgebruikers af op zodanige wijze dat de vertrouwelijkheid ervan niet gecompromitteerd wordt en de afgifte aan de beoogde eindgebruikers is gegarandeerd.

Subscriber
Zie "Abonnee".

Subordinate CA – Sub CA
Een Certification Authority welk onderdeel is van een Certificatiedienstverlener of die onder verantwoordelijkheid van de Certificatiedienstverlener handelt. Bij de PKI voor de overheid wordt het certificaat van de Sub CA getekend met de signing key van de CSP Certification Authority. Zie verder "Certification Authority" en zie ook het plaatje bij "Hiërarchisch model".

Target of Evaluation - TOE
Een product of systeem inclusief de bijbehorende documentatie dat wordt onderworpen aan een evaluatie.

Taskforce PKIoverheid
De projectorganisatie die de 'PKI voor de overheid' heeft gerealiseerd. De Taskforce PKIoverheid heeft op 31 december 2002 zijn activiteiten afgerond.

Tekensleutel
Zie "Signing Key".

Time Stamping Authority – TSA
Een entiteit die een bestaansbewijs levert van een bepaalde datum op een zeker tijdsmoment.

Time Stamping Service – TSS
Een dienst van een CSP die garandeert dat gegevens op een bepaalde datum en tijd zijn aangemaakt of verstuurd.

Time stamping unit

Een verzameling van hardware en software die als geheel wordt beheerd en op een willekeurig moment één enkele Time Stamping Signing key actief heeft.

Toegangscontrolelijst – TCL (E: Access Control List - ACL)
Een lijst die weergeeft wie recht op toegang heeft tot de verschillende (onder-)delen van een PKI systeem. De lijst is daarmee een vorm van autorisatie.
Een TCL wordt voornamelijk gebruikt om te beheren wie toegang heeft tot bestanden en directories op een web server en een directory server.

Token
Een beveiligd stukje hard- of software waarin de private sleutels van de eindgebruiker opgeslagen worden. Een hardware token kan ook cryptografische berekeningen uitvoeren. Voorbeelden van hardware tokens zijn een smartcard en een USB-token.

Trusted Third Party - TTP
Zie "Certification Service Provider".

Trustlist
Een lijst met vertrouwde certificaten of vertrouwde Certification Authorities.

USB-token
Een USB-token is een token vergelijkbaar met een smartcard, maar heeft een andere vorm. Het is een medium om certificaten op te slaan. Het verschil is dat voor een USB-token geen extra smartcardreader hoeft te worden geïnstalleerd. Daarentegen is het niet mogelijk om eindgebruikerkenmerken op de USB-token op de nemen, zoals een foto of persoonsgegevens.

Validiteitsdata
Zie "Validity data".

Validity data (NL: Geldigheidsgegevens)
Aanvullende gegevens, verzameld door de ondertekenaar en/of de controlerende partij, benodigd om de juistheid en geldigheid van een elektronische handtekening te controleren om zo aan de vereisten van de Certificate Policy te voldoen.

Veilig middel voor het aanmaken van elektronische handtekeningen
Zie "Secure Signature Creation Device".

Verifier
Een entiteit die de juistheid en geldigheid van een elektronische handtekening controleert. Dit kan zowel een vertrouwende partij zijn als een derde partij die is geïnteresseerd in de geldigheid van een elektronische handtekening.

Vertrouwelijkheid
De garantie dat gegevens daadwerkelijk en uitsluitend terechtkomen bij degene voor wie zij zijn bedoeld, zonder dat iemand anders ze kan ontcijferen. Buiten de private sector wordt hiervoor ook wel de term "exclusiviteit" gebruikt.

Vertrouwelijkheidcertificaat
Een certificaat waarin de publieke sleutel van het sleutelpaar wordt gecertificeerd dat voor vertrouwelijkheiddiensten wordt gebruikt.

Vertrouwende partij (E: Relying Party)
Een natuurlijke persoon of rechtspersoon die ontvanger is van een certificaat en handelt in vertrouwen op het certificaat.

Virtual Private Network - VPN
Een techniek waarmee een logisch afgescheiden netwerk op een algemeen toegankelijk fysiek netwerk kan worden gebouwd. Deze techniek wordt momenteel veel gebruikt om beveiligd telewerken of flexwerken mogelijk te maken.

Voluntary accreditation
Zie "Vrijwillige accreditatie".

Vrijwillige accreditatie (E: voluntary accreditation)
Een vergunning waarin de rechten en verplichtingen betreffende de verlening van certificatie diensten zijn vermeld en die op verzoek van de betrokken certificatiedienstverlener wordt afgegeven door de openbare of particuliere instantie die is belast met de vastlegging en de handhaving van die rechten en verplichtingen, wanneer de certificatiedienstverlener de uit de vergunning voortvloeiende rechten niet kan uitoefenen zolang hij het besluit van die instantie niet heeft ontvangen. [Europese Richtlijn]

Wet EH
De wet elektronische handtekeningen (Wet EH) die in eerste vorm op 18 mei 2001 aan de Tweede Kamer is aangeboden en op 6 mei 2003, na enige aanpassingen, door de Eerste Kamer is aangenomen. De wet is van kracht sinds 21 mei 2003. Het dossiernummer is 27 743.

Wet op Identificatieplicht (WID)
In de WID is vermeld met welke identiteitsbewijzen de identiteit van personen kan worden vastgesteld.

What Is Presented Is What You See – WIPIWYS
Een beschrijving van de vereiste kwaliteiten van de interface die op ondubbelzinnige wijze het bericht van de eindgebruiker aflevert overeenkomstig de inhoud van het bericht van de eindgebruiker.

What You See Is What You Sign - WYSIWYS
Een beschrijving van de vereiste kwaliteiten van de interface die op ondubbelzinnige wijze garandeert dat hetgeen een eindgebruiker ziet op zijn beeldscherm om te tekenen ook datgene is wat elektronisch van zijn handtekening wordt voorzien.

Witte kaart
Een kaart (met name een smartcard) die nog niet voorzien is van bedrukking of sleutelmateriaal.

X.509
Een ISO standaard die een basis elektronische opmaak voor certificaten definieert.

3 Afkortingen

De volgende afkortingen zijn geldig binnen het document "Programma van Eisen" en de definitielijst. Daar waar het afgekorte begrip een toelichting behoeft, is deze toelichting in de definitielijst opgenomen. Deze begrippen zijn cursief weergegeven.

AA	*Attribute Authority*
ACL	*Access Control List*
AES	*Advanced Encryption Standard*
AID	Application Identifier
API	*Application Programming Interface*
ARL	Authority Revocation List
BM	Biometric Method
BPR	Basisadministratie Persoonsgegevens en Reisdocumenten
BSM	Biometric Sensor Unit
CA	*Certification Authority*
CC	*Common Criteria*
CDSA	*Common Data Security Architecture*
CEN	Comité Européen de Normalisation
CGA	*Certification Generation Application*
CMS	Cryptographic Message Syntax
CN	*CommonName*
CP	*Certificate Policy*
CPS	*Certification Practice Statement*
CPU	Central Processing Unit
CRA	Card Reader Application
CRL	*Certificate Revocation List*
CSP	*Certification Service Provider*
CWA	*CEN Workshop Agreement*
DES	*Data Encryption Standard*
DN	*Distinguished Name*
DPV	Dedicated Path Validation
DS	*Dissemination Service*
DSA	Digital Signature Algorithm
DTBS	*Data to be signed*
EAL	*Evaluation Assurance Level*
EEMA	European Electronic Messaging Association
EEPROM	Electronically Erasable Programmable Read Only Memory
EESSI	*European Electronic Signature Standardization Initiative*
EFT	Electronic Funds Transfers
EN	Europese Norm
eNIK	*elektronische Nederlandse Identiteitskaart*
ETSI	*European Telecommunications Standards Institute*
EVCP+	*Enhanced Extended Validation Certificates Policy*
FIPS	*Federal Information Processing Standard*
GBA	Gemeentelijke Basis Administratie
HSM	*Hardware Security Module*
http	HyperText Transfer Protocol
HW	Hardware
ID	Identifier
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	*Internet Engineering Task Force*

IFM	Interface module
I/O	Input/Output
IP	Internet Protocol
ISO	International Organization for Standardization
KEA	Key Escrow Agency
LCP	*Lightweight Certificate Policy*
LDAP	*Lightweight Directory Access Protocol*
LRA	*Lokale Registration Authority*
MD	*Message Digest*
NAP	Nationaal Actieprogramma Elektronische Snelwegen
NCP	*Normalized Certificate Policy*
NCP+	*extended Normalized Certificate Policy*
NEN	Nederlandse Norm
NIST	National Institute of Standards & Technology
NQC	*Non-Qualified Certificate*
OCF	*Open Card Framework*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
OTAP	Ontwikkel-, Test-, Acceptatie- en Productiesystemen
PA	*Policy Authority*
PnP	*Plug and Play*
PDA	Personal Digital Assistant
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKCS	*Public Key Cryptography Standard*
PKI	*Public Key Infrastructure*
POP	Proof of Possession
PP	*Protection Profile*
PRNG	Pseudo Random Number Generator / Pseudo Random Noise Generator
PUK	*Personal Unblocking Key*
QC	*Qualified Certificate*
QCP	*Qualified Certificate Policy*
RA	*Registration Authority*
RFC	*Request for Comments*
RIPEMD	*Race Integrity Primitives Evaluation Message Digest*
RND	Random Number
RNG	Random Number Generator
RP	*Relying Party*
RSA	*Rivest-Shamir-Adleman*
S/MIME	*Secure Multi-Purpose Internet Mail Extensions*
SCA	Signature Creation Application
SCD	*Signature Creation Device*
SCE	Signature Creation Environment
SF	*Security Function*
SHA	*Secure Hash Algorithm*
SM	Secure Messaging
SOF	*Strength of Function*
SSCD	*Secure Signature Creation Device*
SSL	*Secure Sockets Layer*
SSM	Secured Signature Module
SSO	*Single Sign-On*
Sub CA	*Subordinate CA*
SUD	*Secure User Device*
SVD	*Signature Verification Device*

TCPA	Trusted Computing Platform Alliance
TOE	*Target of Evaluation*
TTP	*Trusted Third Party*
TSA	Time Stamping Authority
TSP	Time Stamp Protocol
TSS	*Time Stamping Service*
TWS	Trustworthy Systems
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VPN	*Virtual Private Network*
WAP	Wireless Application Protocol
WBP	Wet Bescherming Persoonsgegevens
WID	Wet op Identificatieplicht
WIPIWYS	*What Is Presented Is What You See*
WYSIWYS	*What You See Is What You Sign*

4 Revisies

4.1 Wijzigingen van versie 4.1 naar 4.2

Geen wijzigingen

4.2 Wijzigingen van versie 4.0 naar 4.1

4.2.1 Aanpassingen

- In de lijst van erkende beroepen "Accountans-Administratieconsulent" aangepast in "Accountan-Administratieconsulent".

4.3 Wijzigingen van versie 3.7 naar 4.0

4.3.1 Aanpassingen

- In de lijst van erkende beroepen "alle medici" geschrapt en opgenomen een verwijzing naar een wettelijk register (ingangsdatum 4 weken na publicatie PVE 4.0)

4.4 Wijzigingen van versie 3.6 naar 3.7

Geen wijzigingen.

4.5 Wijzigingen van versie 3.5 naar 3.6

4.5.1 Aanpassingen

- Geschrapt "Waarnemend notaris" en opgenomen "Toegevoegd notaris" (ingangsdatum 4 weken na publicatie PVE 3.6)

4.5.2 Redactioneel

- Bevoegd vertegenwoordiger: Commissaris van de Koning (ingangsdatum 4 weken na publicatie PVE 3.6);

4.6 Wijzigingen van versie 3.4 naar 3.5

Geen wijzigingen

4.7 Wijzigingen van versie 3.3 naar 3.4

4.7.1 Nieuw

Niet van toepassing.

4.7.2 Aanpassingen

- Kandidaat notaris op genomen in de lijst van erkende beroepen.

4.7.3 Redactioneel

Niet van toepassing.

4.8 Wijzigingen van versie 3.2 naar 3.3

4.8.1 Nieuw

- Definitie van publiek en privaat IP adres

4.8.2 Aanpassingen

- Definitie van Fully Qualified Domain Name.

4.8.3 Redactioneel

Niet van toepassing.

4.9 Wijzigingen van versie 3.1 naar 3.2

4.9.1 Nieuw

Niet van toepassing.

4.9.2 Aanpassingen

- Definitie van Beroepsgebonden certificaathouder.

4.9.3 Redactioneel

Niet van toepassing.

4.10 Wijzigingen van versie 3.0 naar 3.1

4.10.1 Nieuw

- Definitie van Multi-factor authenticatie en Reseller.

4.10.2 Aanpassingen

Geen wijzigingen.

4.10.3 Redactioneel

Niet van toepassing.

4.11 Wijzigingen van versie 2.1 naar 3.0

4.11.1 Nieuw

- Definitie van Autonome Apparatencertificaat, Beroepsgebonden certificaten, Bevoegd vertegenwoordiger, Enhanced Extended Validation Certificates Policy – EVCP+, Extended Validation SSL certificaten, Generiek TopLevelDomein (gTLD), Land code TopLevelDomein (ccTLD), Organisatiegebonden certificaten, Overheid, Persoonsgebonden certificaten en Services certificaat

4.11.2 Aanpassingen

Geen wijzigingen.

4.11.3 Redactioneel

Niet van toepassing.

4.12 Wijzigingen van versie 2.0 naar 2.1

4.12.1 Redactioneel
Alleen een aantal redactionele aanpassingen zijn doorgevoerd maar deze hebben geen gevolgen voor de inhoud van de informatie.

4.13 Wijzigingen van versie 1.2 naar 2.0

4.13.1 Nieuw
Niet van toepassing.

4.13.2 Aanpassingen
Geen wijzigingen.

4.13.3 Redactioneel
Niet van toepassing.

4.14 Wijzigingen van versie 1.1 naar 1.2

4.14.1 Nieuw
Geen wijzigingen.

4.14.2 Aanpassingen
Geen wijzigingen.

4.14.3 Redactioneel
Een aantal redactionele aanpassingen zijn doorgevoerd maar deze hebben geen gevolgen voor de inhoud van de informatie.

4.15 Wijzigingen van versie 1.0 naar 1.1

4.15.1 Nieuw
- Definitie van Fully Qualified Domain Name (FQDN).

4.15.2 Aanpassingen
Geen wijzigingen.

4.15.3 Redactioneel
Geen wijzigingen.

4.16 Versie 1.0
Eerste versie.